

L Number	Hits	Search Text	DB	Time stamp
1	0	account with (name or number) with randomly with generat\$4 with password	EPO; DERWENT	2003/06/30 15:13
4	0	account with (name or number) with randomly with generat\$4 with password	EPO; DERWENT	2003/06/30 15:13
7	0	account with (name or number) with random\$3 with generat\$4 with password	EPO; DERWENT	2003/06/30 15:13
10	1	account near (name or number) same random\$3 with generat\$4 with password	EPO; DERWENT	2003/06/30 15:14
13	6	account near (name or number) same random\$3 with generat\$4 with password	USPAT; US-PGPUB	2003/06/30 16:13
16	421	random\$3 with generat\$4 with password	USPAT; US-PGPUB	2003/06/30 17:33
19	2	16.ti.	USPAT; US-PGPUB	2003/06/30 15:27
22	24	16.ab. not 16.ti.	USPAT; US-PGPUB	2003/06/30 15:27
25	289	random\$3 with generat\$4 with pin	USPAT; US-PGPUB	2003/06/30 15:34
28	0	25.ti.	USPAT; US-PGPUB	2003/06/30 15:34
31	18	25.ab.	USPAT; US-PGPUB	2003/06/30 15:34
34	1	"5130519".PN.	USPAT	2003/06/30 15:38
35	1	"5130519".PN.	USPAT	2003/06/30 15:38
36	19	5265162.URPN.	USPAT	2003/06/30 15:38
45	86	portable same random\$3 with generat\$4 same (pin or password)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/06/30 16:14
52	3726	portable with (pin or password)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/06/30 16:14
59	161	portable near (pin or password)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/06/30 16:16
66	5	(portable near (pin or password)) and random\$3 near (pin or password)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/06/30 16:15
73	5	portable near (pin or password) near2 storage	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/06/30 16:24
80	1	wo-8702491-\$.did.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/06/30 17:26
87	1171	prompt with user with password	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/06/30 17:28
94	8	(prompt with user with password) same random\$4 with password	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/06/30 17:26
101	0	prompt with user with password with randomly	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/06/30 17:28

108	1	prompt with user with (pin or password) with randomly	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/06/30 17:28
115	6	prompt near user near new near (pin or password)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/06/30 17:29
122	104	random\$3 near generat\$4 near (pin or password)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/06/30 17:35

(12) UK Patent Application (19) GB (11) 2 181 582 (13) A
(43) Application published 23 Apr 1987

(21) Application No 8624291

(22) Date of filing 9 Oct 1986

(30) Priority data

(31) 8525161

(32) 11 Oct 1985

(33) GB

(71) Applicant

Victor Campbell Blackwell,
69 Westminster Drive, Bromborough, Wirral,
Merseyside L62 6AN

(72) Inventor

Victor Campbell Blackwell

(74) Agent and/or Address for Service

Potts Kerr & Co., 15 Hamilton Square, Birkenhead,
Merseyside L41 6BR

(51) INTCL⁴

G07F 7/08

(52) Domestic classification (Edition I)

G4H 13D 14A 14B 1A TG

(56) Documents cited

GB A 2131992	GB	1595796
GB A 2129176	GB	1505715
GB A 2120434	GB	1422217
GB A 2114791	EP A1	0086286
GB A 2100897	WO A1	85/04035
GB A 2092343	WO A1	83/03018
GB A 2069201	US	4529870
GB A 2016768	US	4459474

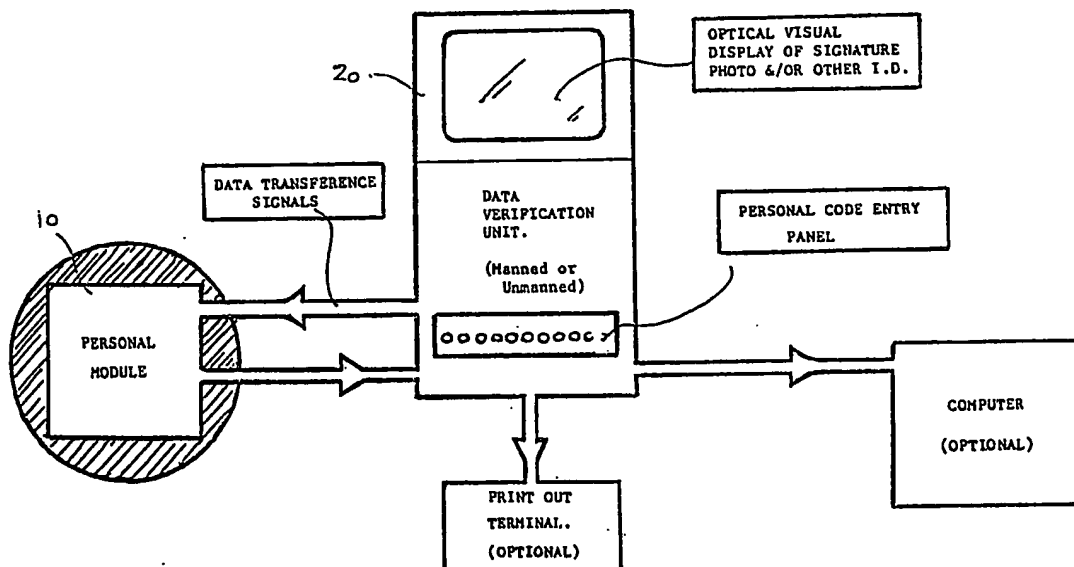
(58) Field of search

G4H

Selected US specifications from IPC sub-classes G07F
G06K

(54) Personal identification device

(57) An electronic device for enabling the output of personal identity information includes secure storage means for storing said personal identity information, accessible upon actuation either by equipment capable of communicating with the device or by display to the user for input to equipment to which access is sought.



PERSONAL I.D. MODULE IN VERIFICATION MODE.

Fig. 2

GB 2 181 582 A

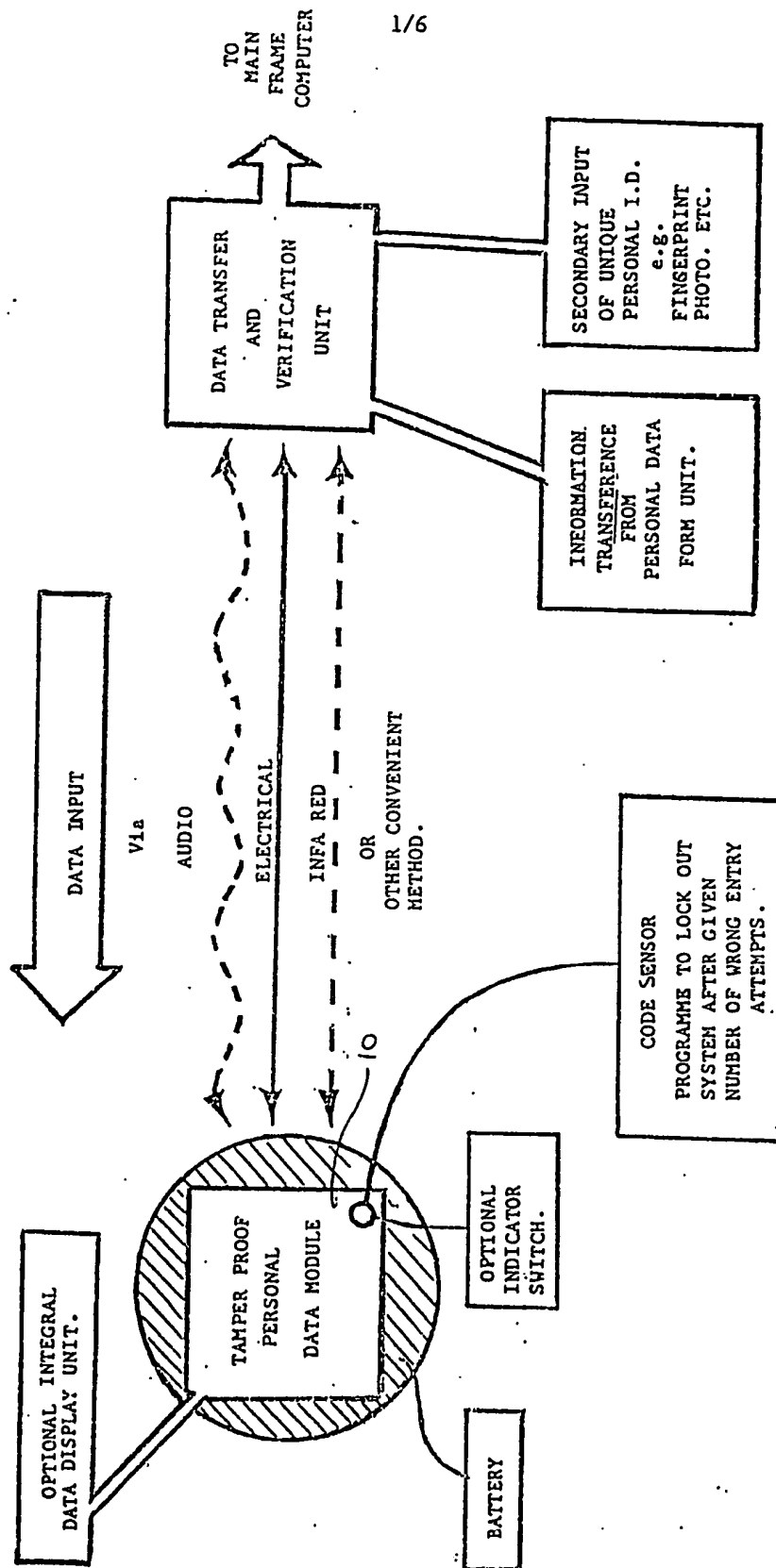


fig 1

DATA LOADING MODE.

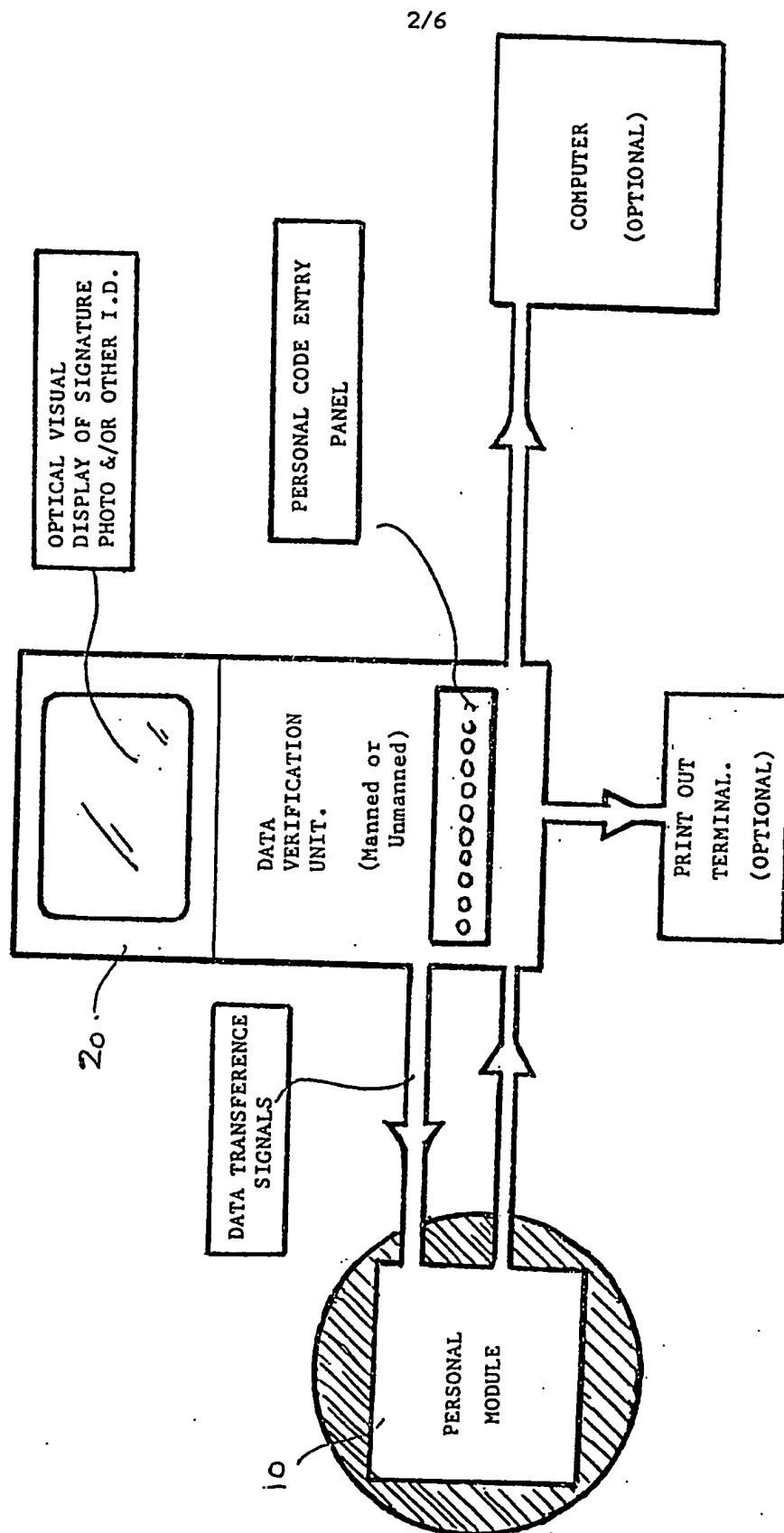
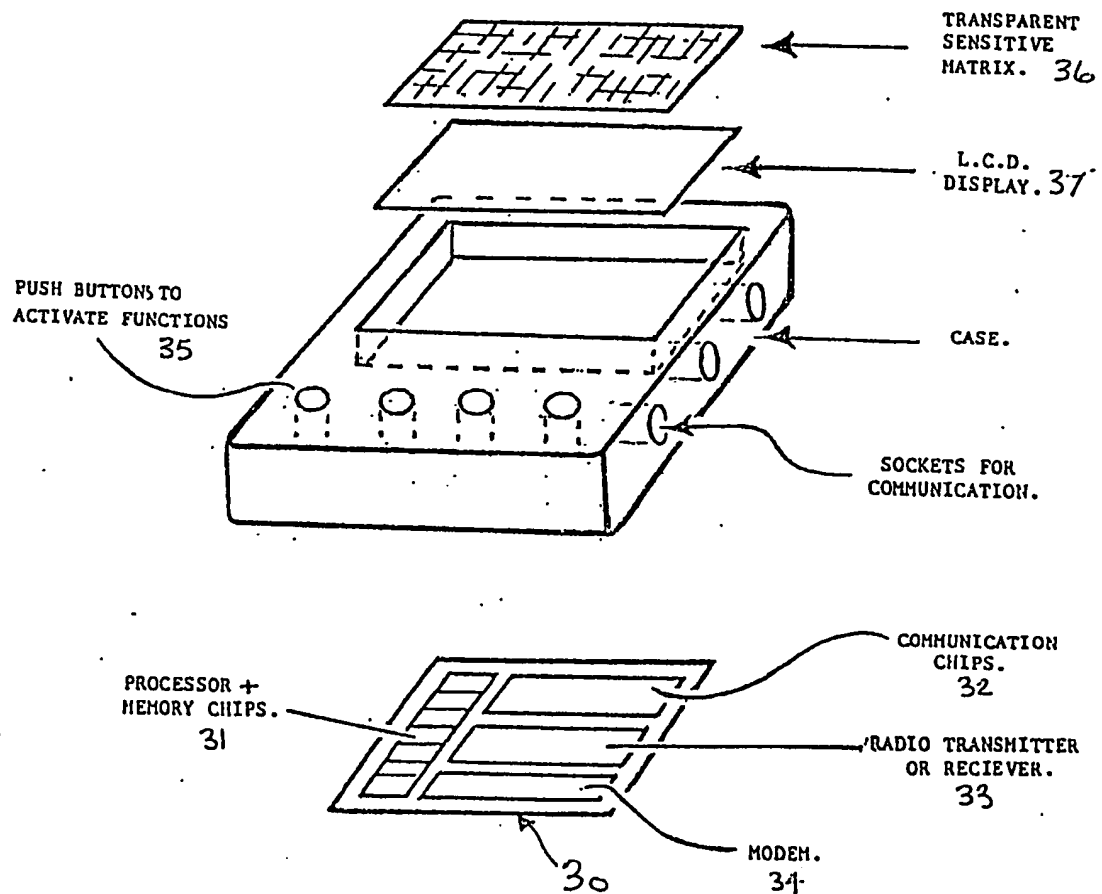
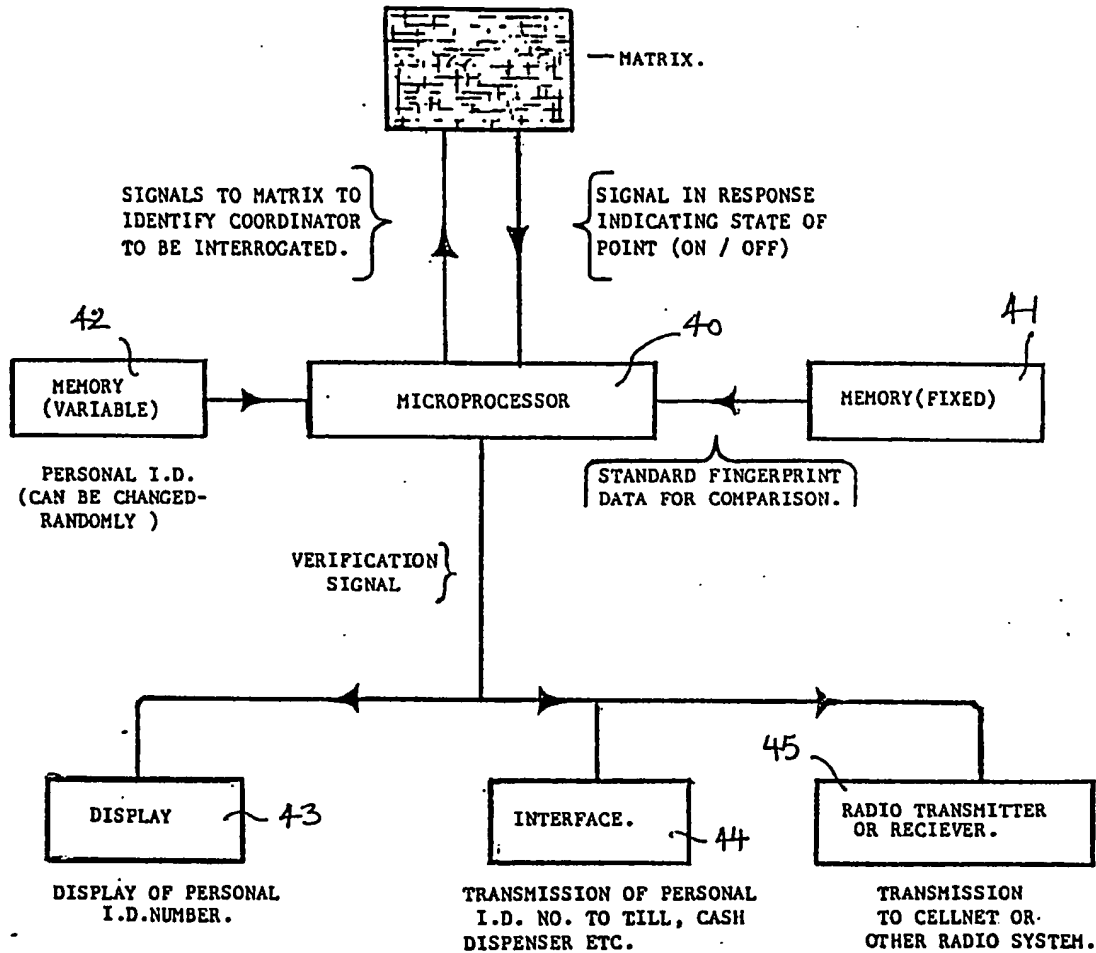
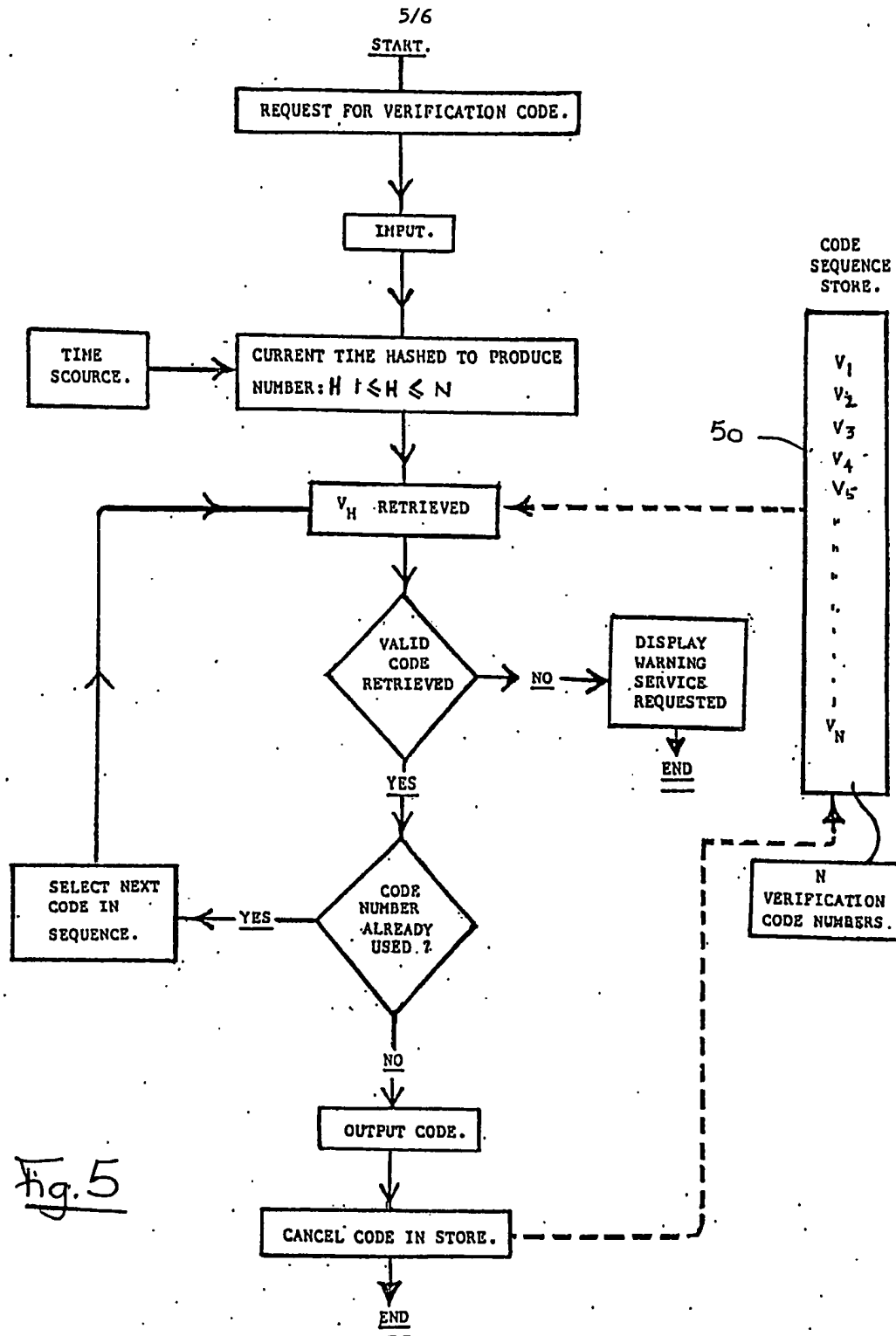


Fig. 2

PERSONAL I.D. MODULE IN VERIFICATION MODE.

Fig. 3

Fig 4



2181582

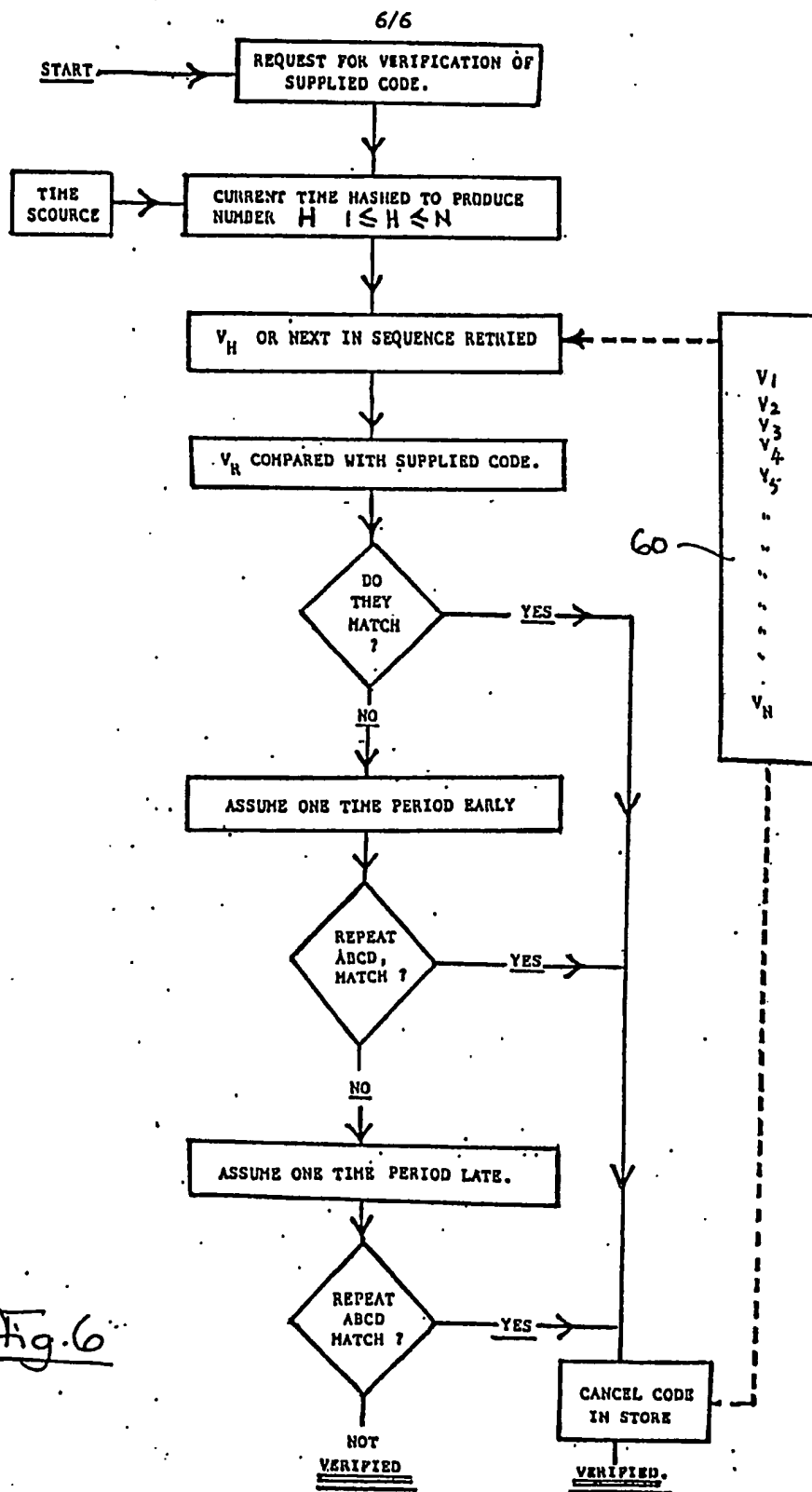


Fig. 6

SPECIFICATION

Personal identification device

5 The present invention relates to a personal identification device which can enable an individual to provide proof of identity or enable validation of an individual's right of access to various facilities, which may additionally incorporate storage means for a variety of personal information about the individual.

10 A variety of different types of identification devices are known, some of these being in the form of security passes, wherein an access code is stored on a card, and in the form of a magnetic strip or a combination of magnetized dots or in the form of optical character readable print. Such cards may additionally include one or more photographs of the holder and the holder's name, signature, status etc. Further, credit cards, charge cards or cash cards are known which enable a user to access a bank computer in order to withdraw money from their current account or to obtain cash advances from a credit account, or to obtain goods and services from retailers or restaurants or the like. Such cards are normally issued by banks and other financial institutions to allow their customers access to a range of services provided for them. In addition, independent credit card companies also exist and a variety of large chain stores and mail order stores have their own credit card schemes, so that there is a potential for an individual to have dozens of different cards available to him. With many of these cards, particularly those issued by banks, a customer can obtain a personal identification number (p.i.n. code) for use with a particular banks card for use when obtaining access to his own account or accounts at the bank or for making cash withdrawals or other financial transactions. In view of the large number of cards which utilise such a p.i.n. code, the user may have to remember several different p.i.n. codes for different accounts which he holds. The p.i.n. code is essential with such devices to assure security of access to an individual user's account, since the card and correct p.i.n. number are required before the card can be utilised in accessing the information via a cash dispenser or service till.

It is a disadvantage of the present type of devices that each company issuing a card utilises their own coded information on the card for identifying the account of the user, which is then confirmed by the user by input of the correct p.i.n. code, so that existing cards are not fully interchangeable with cards of another supplier and because of the large numbers of cards which may be involved, a user may have to attempt to remember several p.i.n. numbers for the various cards held. The result of this problem is often that the user of the card, despite warnings from the company issuing the card, will often write down the p.i.n. number on something carried with the card, so that in the event the number is forgotten the number can be looked up readily. Unfortunately, this does cause security problems in that, if the card is stolen, it may be that the security number will also have been stolen, thereby giving the thief immediate access to the card holder's personal account.

In order to overcome such a problem, it would be preferable to attempt to provide a single device, which is capable of being utilised by all users and which contains universally acceptable information about the user for enabling correct identification of the user and which at most requires the user to remember a single p.i.n. number but may alternatively utilise another type of personal information, for example, a unique fingerprint or voice print of the user, in order to establish identity for access to secure information or accounts, utilising existing terminal equipment with suitable minor modifications where necessary.

It is the aim of the present invention to seek to provide a personal identity device which may suitably be used as or incorporated in an item of jewellery, or alternatively may be incorporated in a wristwatch, pocket-watch or calculator, according to the user's preference, and which is capable of enabling establishment of the identity of the user.

According to the present invention there is provided an electronic identity device including means for enabling output of identity information upon activation thereof.

Preferably, the output of identity information is time-dependent and said means comprises a multi-number time-dependent code generator synchronised with an identical, remote code generator capable of confirming the identity of the device and the user thereof in a secure system, upon input of a personal identity access code or a personal characteristic of the user. The personal identity access code may be a conventional p.i.n. number which may be input into an electronic console or may comprise a personal characteristic of the user, e.g. a fingerprint or voice print.

Further preferably, the device may also include stored therein various non-secure items of information such as the specific medical history of the user, giving details of any special medical requirements in an emergency, i.e. blood group, allergies etc., which may be suitably accessed in an emergency. The device may also include other personal information such as driving licence number, insurance certificate number and insurance details of the owner's vehicle etc., or the passport number and an image of the user which may either be displayed on the device itself or be transmitted via a suitable link to a console for display of such information as required, e.g. for a customs or immigration official.

The device of the present invention may suitably be incorporated in an item of jewellery such as a wristwatch, pendant or bracelet or the like or in a pocket electronic calculator or travel alarm clock and may include its own display or be connectable to or capable of communicating with another device such as a compatible terminal in a bank or other establishment for the display of information. The device may include long-life batteries or may utilise solar cells or a combination of these to prolong useful life thereof if required, but the device is preferably provided as a sealed secure unit having a predetermined life, so that secure information may only be input to the device initially and may not subsequently be altered or updated, although separate means may be provided

for input and update of non-secure information, as referred to above.

The device of the present invention provides a useful identity device, which is less likely to be lost or misplaced than identity cards or bracelets or credit cards or the like and which is capable of storing a variety of information, including emergency information about the wearer in a single device, which may be used for a variety of purposes, including entry access to a vehicle security system or home security system belonging to the user. The device could also include or activate a small transmitter for the output of a signal for operating equipment remotely from the device, e.g. for disarming a security system or opening a security door or the like or for communicating directly with a radio telephone network to enable transactions to be performed at a variety of locations, for example, by suitable interfacing with a cellular telephone device. Similarly, such devices may be used additionally as a paging device to enable the wearer to be contacted whatever his location may be again utilising the cellular telephone network.

Depending upon the intended usage of device, such may be provided with, or connectable to, an appropriate keyboard module to enable such to be used as a data storage means or possibly a display for another device such as a calculator or even connectable to a portable computer.

The device may include a tamper-proof arrangement which would act to prevent access to the secure identity information or unauthorised output of information, other than emergency information which may be required.

The present invention will now be described further, by way of example, with reference to the accompanying drawings, in which:-

Figure 1 illustrates schematically, a module according to the present invention;

Figure 2 illustrates a possible example of the module of *Figure 1* in use with a verification console; *Figure 3* illustrates a possible construction of a module according to the present invention and utilising a sensitive matrix for scanning a fingerprint applied thereto;

Figure 4 is a block diagram of a possible circuit for performing the function of the present invention when utilising a fingerprint as identification means;

Figure 5 illustrates the internal program of a time dependent code generating device incorporated in a device of the present invention; and

Figure 6 illustrates the corresponding program steps in a remote device capable of being linked with a module utilising the program set out in *Figure 5*.

Referring firstly to *Figure 1*, an example of a personal data module device 10 is shown schematically illustrating the manner in which the device 10 may be loaded with information upon commissioning thereof for a particular user, including personal account information and details for establishing the identity of the user, including a personal characteristic or a p.i.n. code. In addition, the user may be allowed to input personal data, either by supplying such information to the institution issuing the device 10, or via a console supplied with the device, or on a keypad incorporated in, or able to communicate

with, the device.

The relevant information stored in the device 10 can be stored in a central computer unit of the institution issuing the device so that, at a subsequent date, when the device is activated and is in communication with a peripheral connected to the institution's central computer of the institution, e.g. a bank, the user is able to access personal account details etc. and update and make requests of the central computer.

Alternatively, the device 10 could simply communicate with a console, which may be manned, such console being capable of producing a visual display 20, as shown in *Figure 2*, which can display to the operator personal information about the holder of the module in order to establish the identity thereof, for example the signature, photograph, or other personal information about the user which the operator can utilise to verify his identity.

As can be appreciated from the above, there are a variety of applications in which the module can be used whether used by a bank teller, or retailer dealing directly with the customer, or via an automatic till or cash dispenser or the like.

As referred to above, the device is preferably incorporated in a watch, since such may already contain much of the circuitry necessary for performing the functions of the device, namely a microprocessor and associated program storage and data storage means and a liquid crystal display. Relatively complex watches are available which include storage facilities and indeed which are connectable to computer devices to enable uploading and downloading of information therefrom and may act as a display device for a miniature computer or calculator. As such therefore, many of the functions of the watch as envisaged by the present invention can be readily combined from existing devices, but additionally includes a secure personal p.i.n. code, known only to the user, or personal characteristics of the user, for example, the characteristics of the fingerprint or voice print of the user which can be used to activate the secure operation of the device, when seeking access to sensitive installations, not only including personal bank information relating to the user, but also for general security purposes, if desired. Once correctly actuated by such secure means, the device can then be utilised by such secure means, the device can then be utilised to enable access to such secure installation or equipment by transmission of a code signal unique to the device and recognisable by the security equipment controlling access to such information or installation, such secure code being able to be transmitted directly thereto by any of a variety of means, including an ultrasonic or infrared signal or a direct electrical link to the equipment or by a short range radio transmission. As an alternative to incorporating such features in the watch itself, the means for inputting the personal identity number or the voice or fingerprint could be contained within the console of the equipment with which the device is communicating such that on actuation of the device by a non-secure means, the installation being sought to be accessed identifies the specific watch in question and awaits a confirmation by means of the input of a personal code into the machine itself or by the applic-

ation of a recognisable thumb print or fingerprint or upon recognition of the required voice matching the voice print stored by the computer. As such, therefore the device itself requires very few component parts, the bulk of the recognition system being contained within the console, rather than the wrist watch thereby enabling simplification of the construction of the device.

Referring now to Figure 3, this illustrates in an exploded view a possible construction of a wrist watch in which the electronic circuitry is contained on a PCB 30 containing the necessary electronic circuitry in micro-electronic form, including the normal watch or clock function devices together with micro-processor and memory storage chips 31 and devices 32 for enabling communications, either by utilising an on-chip transmitter and/or receiver 33 and possibly a modem 34, enabling the device to be utilised in communication with other devices down a cable connector, or via an antenna which is preferably formed by the bracelet of the watch. In addition, a transparent matrix 36 overlies an LCD display 37 in order to detect the conformation of a fingerprint applied thereto. Suitable buttons 35 may be provided on the watch case to enable actuation of the device and for control of the various clock functions in order to enable other functions, which may be required of the watch, to be performed.

Referring now to Figure 4, this is a block circuit diagram illustrating the manner in which the components can be connected together to perform the function as described above in the embodiment of a watch having a pressure sensitive matrix for detecting a fingerprint applied thereto. In the arrangement shown in Figure 4, the device is controlled by a microprocessor 40 with associated fixed or read-only memory 41 for storing secure details including data relating to the configuration of the fingerprint of the user for comparison with the configuration of the fingerprint applied to the matrix upon actuation of the device. In addition, a variable or updateable memory 42 can additionally be provided to store information which is likely to be changed from time to time, for example any personal information. The microprocessor 40 also controls the normal clock functions of the watch, details of which are not shown, but are standard in the art, as well as controlling enabling of the display 43 or any of the various interfaces 44 or radio transmitter and receiver 45 according to which are provided in the device. For example, the display 43, in addition to being able to display the normal time and various clock functions as per a standard watch, such can store other i.d. information or personal details, according to the purposes to which the device is to be applied, including any messages which may have been received by the device if such is used in a radio reception mode, for example for radio paging or the like via the cellular telephone network. Alternatively, the display 43 of the watch may only display the clock functions, the security aspects of the device being achieved by transmission of appropriate coded information to a console via a short range ultrasonic or infrared or radio transmission or via a direct local connection by a short lead to a device with which it is to communicate. The particular

manner in which the device would function in practice would be determined entirely by the intended use and the desired features to be incorporated. For the purpose of direct connection or facilitating radio transmissions or ultrasonic infrared signals to be transmitted, then appropriate interfaces and receivers are supplied again controlled by the microprocessor 40, as required.

It is considered that in one possible embodiment, as far as the user is concerned, the device performs only normal functions of a watch or other device in which the device of the present invention is incorporated, with all the necessary communication with security systems being performed in a manner not apparent to the user, so as to avoid complicating the device, the user only being required to make appropriate input to a console with which the device is to communicate, in which case the various more complex pieces of apparatus which may be required for use with the device can be incorporated in the console. For example, upon actuation of the device, a signal is transmitted to the console to identify the user and then confirmation of the identity of the user is input by the user directly into the console, i.e. either by applying his fingerprint to a designated part of the console, so that such may be scanned, or by inputting a personal identity number, or for example by speaking into the console or by writing his signature on a sensitive portion of the console, or by any suitable other alternative means, which may be considered to be a suitable unique personal characteristic to confirm identity of the user before access is permitted to the facilities of the console or into a secure location.

As it will be appreciated, all of such facilities may be provided on the device itself or be provided on a further device connectable to the device of the invention. A further alternative which is envisaged is the use of a video card or disc in which the information is permanently stored thereon and which is associated with the device of the invention to confirm identity and to minimize the amount of storage required in the device itself, such video disc or card being incorporated in the device, if necessary, possibly forming part of the casing or accommodated therein.

Referring now to Figures 5 and 6, these illustrate flow diagrams of a secure method of identifying a device according to the present invention, in which a matched pair of modules 50, 60 are provided, each being constructed from appropriate memory devices and being programmed with an identical sequence of code numbers, said sequence being generated at random. The pair of modules are readily identified both internally and externally to ensure that these are correctly matched when used. One of such modules 50 is then incorporated in the device of the present invention and another of such modules 60 is incorporated in a central computer of the institution issuing the device. The sequence of numbers in the modules 50 and 60 constitutes a list in which one of said numbers in said list is current for a predetermined period of time, such that at the same time the two numbers in the two modules are identical. Thus, if the module 50 contained in the device of the present invention is interrogated and the number provided

thereby is compared with the number currently in the matched module 60 in the central computer, such numbers will be identical and the device will be uniquely identified. Since such sequences of numbers are generated at random for each matched pair of devices, the likelihood of another similar device producing the same number at the same moment in time, although it is statistically possible, would be infinitesimally small.

Thus, the user of the device, upon actuation thereof, could either have the internal code number current in the list displayed on his device, or transmitted directly to the console so that upon input thereof into the console together with other means of confirming his identity, for example using a p.i.n. number, fingerprint, voice print or other personal characteristic, the identity of the user can be confirmed. The module 60 in the central computer will have meantime indicated to the data base of the institution the correct identity of the user of the device having that code number at that particular moment in time allowing for any transmission delays, etc., and will have looked for confirmation of the identity of the user by appropriate input either into the device of the user or into a console, such as a cash dispenser or service till before permitting access to the facilities thereof. When correct identification has been confirmed, the number used is deleted from the list in the code sequence, so that such cannot be used again, thereby preventing the possibility of anyone attempting to memorise the number and determining the cycle time of the device and thereby attempting to reuse that number. This feature also provides an in-built obsolescence of the device, so that a fresh module can be issued periodically providing an additional degree of control over the use of such modules by the institution.

The generalised program steps required for performance of the necessary routines internally in the device of the present invention and in the central computer containing access to the personal account information etc. are shown in the flow diagrams of Figures 5 and 6.

In addition to the envisaged uses in a bank environment other financial institutions could also utilise such a system, since many building societies are now operating cash dispensers and service tills, and it may be that such a system could constitute the basis of an electronic identity card, which can be used by the security services for unequivocally identifying an individual. In this sense, it is envisaged that such may be of particular value in the area of passport control, with the personal information, including a photographic image of an individual, stored in a central computer and accessed as required by customs officials in order to establish the identity of the user of the device, but such arrangements would require international agreement in order to permit widespread use of such a system.

A further application into which the device of the present invention may be used is in electronic fund transfer at point of sale (eftpos), so that any transaction made by the user would involve such a device,

so that monies could be deducted either from a credit account of the user, or directly from a current account; access to the users personal account being available via a suitable terminal in the retailers premises. Such an embodiment could lead to an arrangement providing an effectively cashless society, which would give considerable central control, which might not always be welcomed by the general public, over cash flow in the economy, in that such information would not only be available to the institutions providing the use of facilities, but could also be made available to tax authorities. This would enable a considerable reduction in "cash only transactions" and provide a considerable hurdle to the black economy, at least from the point of view of supply of materials and equipment, and such could have considerable economic effect.

Further, with the advent of computers across a wide spectrum of society, with a suitable interface, such a device could also provide the user with access to his personal account directly from a home console or home computer, providing the user with much greater control over his accounts and enabling him to perform transactions at home rather than having to visit a banks premises and having to rely upon the issuance of statements, etc, to check the status of his account. Therefore, such a device could provide the user with considerable benefits and a greater degree of flexibility and control over his own personal affairs. Indeed, the user could use such computer-based facilities for purchasing items or booking facilities such as theatre tickets etc. from home, having the appropriate amounts deducted directly from his own personal account similar to the facilities which already exist via PRESTEL in the U.K.

As will be appreciated from the above, the device of the present invention has considerable advantages over existing prior art devices and it provides for a wide range of alternative services and facilities to be provided to the user, who will also have greater degree of control over his own personal financial affairs.

Whilst the device of the present invention is preferably incorporated in a wrist watch, this being an item which virtually everyone possesses and is often the first item put on in the morning and the last item taken off at night, and provides the ideal basis for incorporation of the device of the present invention, since it already contains many of the components necessary for performance of the functions thereof, the device could equally be incorporated in any other personal item, including a personal calculator or an item of jewellery according to preference.

Further, such a device, as envisaged by the invention, may be used with existing credit cards but using the device in a watch to display or transmit coded information to be used in conjunction with the information on the credit card and p.i.n. number to provide a further degree of security over existing arrangements.

CLAIMS

1. An electronic identity device including means for enabling output of identity information upon activation thereof.
2. A device as claimed in claim 1 wherein said enabling means includes means for receiving and comparing input information with data stored in said device and only outputting said identity information upon a correct match between said input information and said stored data being achieved.
3. A device as claimed in claim 1 or 2, in which said input information is selected from either a personal identity number, or an individual characteristic of a user, such as a fingerprint, voice print, signature, or other unique personal characteristic.
4. A device as claimed in any preceding claim wherein said output information is displayed on said device.
5. A device as claimed in any preceding claim wherein said output information is transmitted via ultrasonic, infrared, short range radio transmission, or via an electrical connector to a remote console, in order to enable access to facilities thereof upon confirmation of the identity of the user in a secure manner.
6. A device as claimed in claim 5 in which the identity information is time-dependent and is generated in a multi-number, time-dependent code generator synchronised with an identical, remote code generator associated with central data storage means, with which communication is possible via a console to which access may be sought, so that the module in said device is uniquely identified and, upon confirmation of the identity of the user by means of a personal identity number or personal characteristic, access to the console and thus the central computer system is enabled.
7. A device as claimed in claim 6 in which the time-dependent identity information is either displayed on the device or transmitted directly by said device via an infrared, ultrasonic, short range radio signal or an electrical signal to a remote console to which access is sought in use.
8. The device as claimed in any preceding claim wherein said device additionally contains memory storage means enabling the storage of personal data in a non-secure manner and able to be accessed and updated by the user, by a key pad incorporated in the device or connectable thereto.
9. A device as claimed in any preceding claim, wherein such is incorporated in a watch, preferably a wrist watch.
10. A system for enabling the identification of individuals, comprising a personal electronic identity device including means enabling output of personal identity information for input to a console associated with, or directly to, a computer-based system to enable unique identification of the user of the personal identity device by means of said output information, corroborated by the input to said computer of a personal identity number or the identification of a personal characteristic of the user, to allow access to facilities provided by said computer based system.
11. A system as claimed in claim 10 in which the

output of identity information is time-dependent and each personal identity device incorporates a multi-number code generator matched with an identical, remote code generator associated with the computer for uniquely identifying a particular device at a precise moment in time.

12. A system as claimed in claim 10 or 11 in which said device may interface the computerised system via remote consoles or via a home computer or a telephone link.

13. A device as claimed in any preceding claim in which a radio paging means is incorporated and which may additionally permit full duplex operation allowing the reception or transmission of messages to and from said device.

14. A device as claimed in any preceding claim in which additional devices may be attached thereto in order to access information contained within said device or to provide additional storage or data for access by said device.

Printed for Her Majesty's Stationery Office by
Croydon Printing Company (UK) Ltd, 3/87, D8991685.
Published by The Patent Office, 25 Southampton Buildings, London, WC2A 1AY,
from which copies may be obtained.